



FIG. 1
PRIOR ART

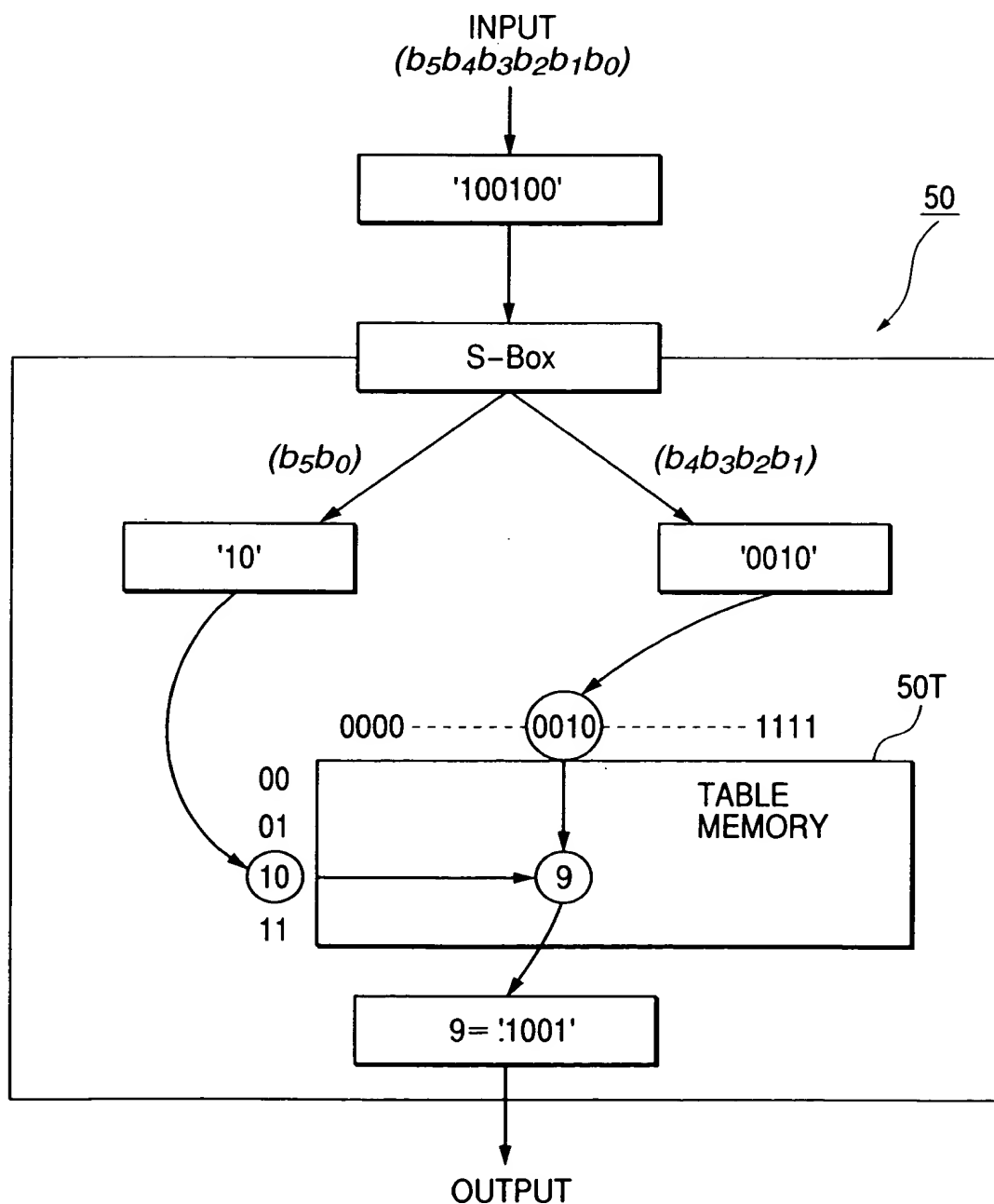
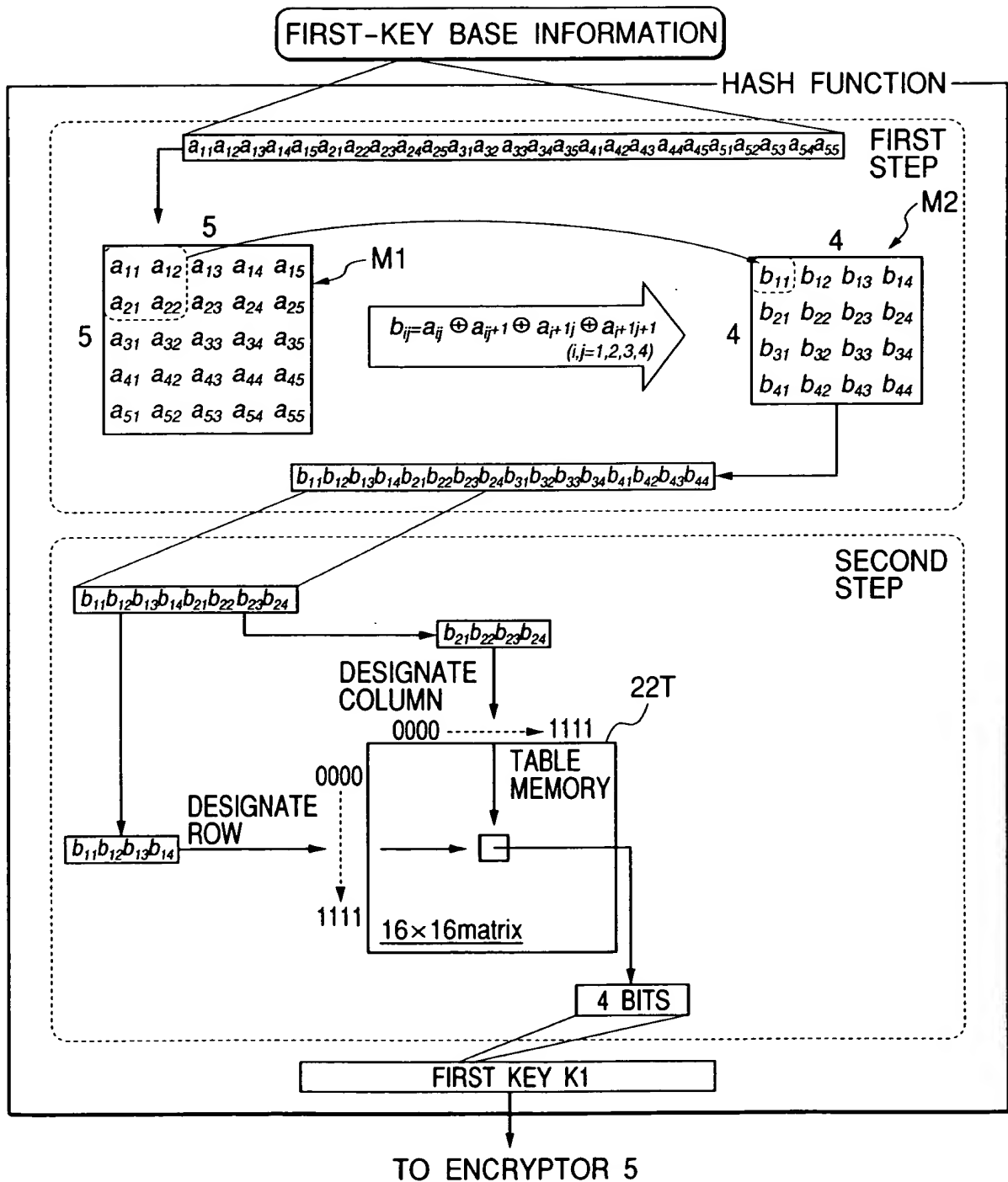


Figure 1 is a block diagram of a cryptographic system, divided into two main sections by a vertical dashed line. The left section, labeled 'P' with a wavy arrow, shows the encryption process. It starts with 'FIRST-KEY BASE INFORMATION' (2) and 'SECOND KEY K2' (1) as inputs to an 'ENCRYPTOR'. The output of the 'ENCRYPTOR' goes to 'ENCRYPTION-RESULTANT FIRST-KEY BASE INFORMATION'. This information then passes through a 'CALCULATOR ONE-WAY FUNCTION' (3) to produce 'FIRST KEY K1' (5). The right section, labeled 'Q' with a wavy arrow, shows the decryption process. It starts with 'DIGITAL CONTENTS INFORMATION' as input to an 'ENCRYPTOR'. The output of the 'ENCRYPTOR' goes to 'ENCRYPTION-RESULTANT DIGITAL CONTENTS INFORMATION'. This information then passes through a 'CALCULATOR ONE-WAY FUNCTION' (10) to produce 'FIRST KEY K1' (11). The 'FIRST KEY K1' (11) is then used as an input to a 'DECRYPTING DEVICE' (11), which also receives 'SECOND KEY K2' (8) as an input. The output of the 'DECRYPTING DEVICE' (11) is 'DIGITAL CONTENTS INFORMATION'. The 'FIRST KEY K1' (5) from the left section is also used as an input to the 'DECRYPTING DEVICE' (11). The 'FIRST KEY K1' (11) is also used as an input to the 'DECRYPTING DEVICE' (11). The 'FIRST KEY K1' (11) is also used as an input to the 'DECRYPTING DEVICE' (11).



FIG. 3





4 / 7

FIG. 4

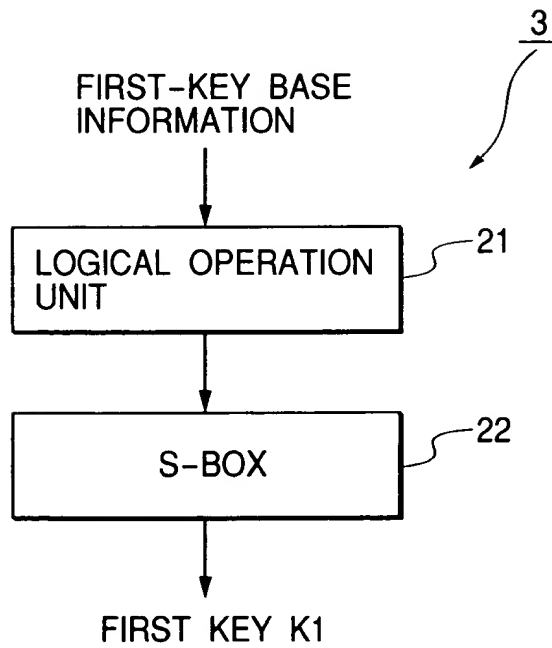


FIG. 5

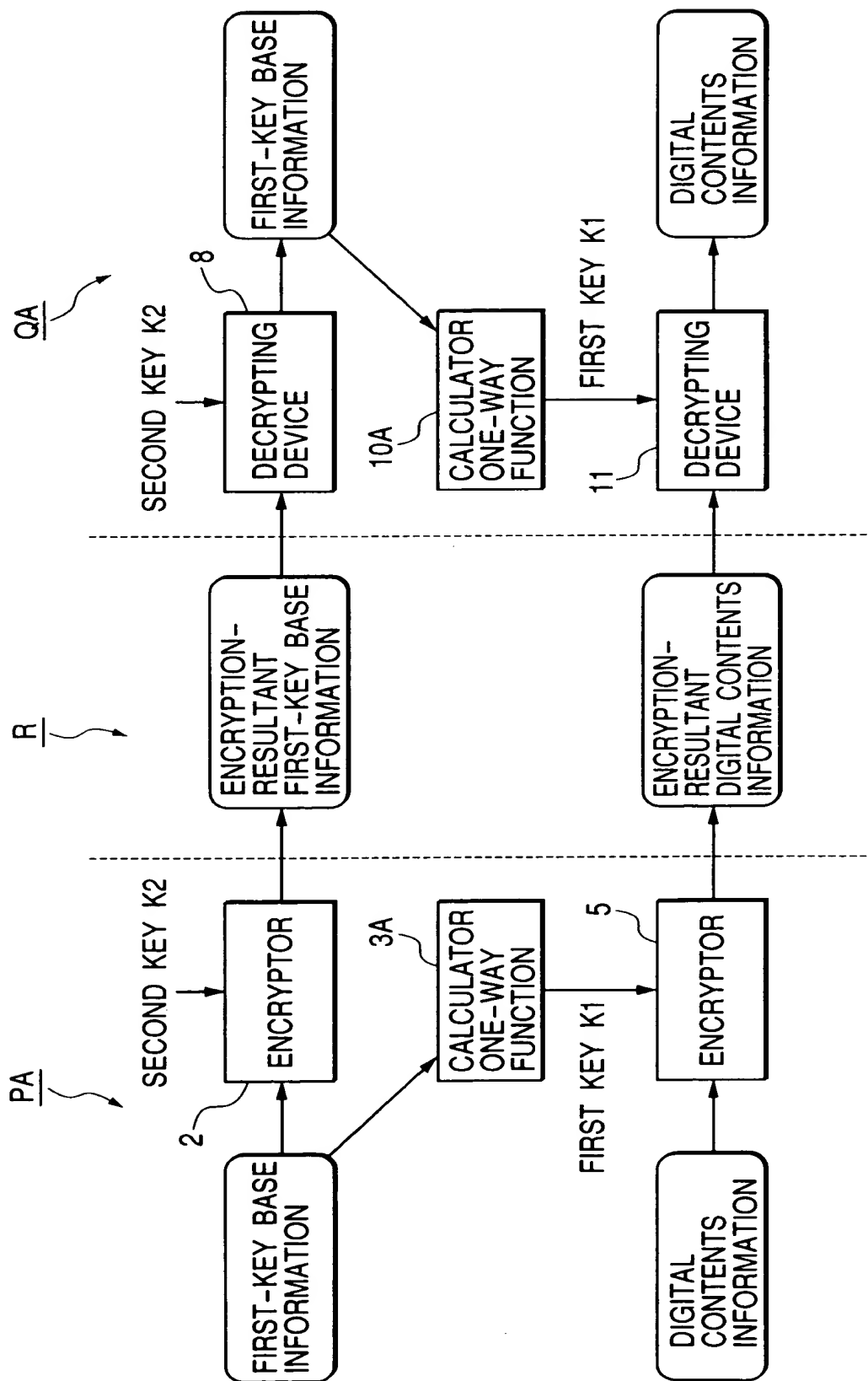
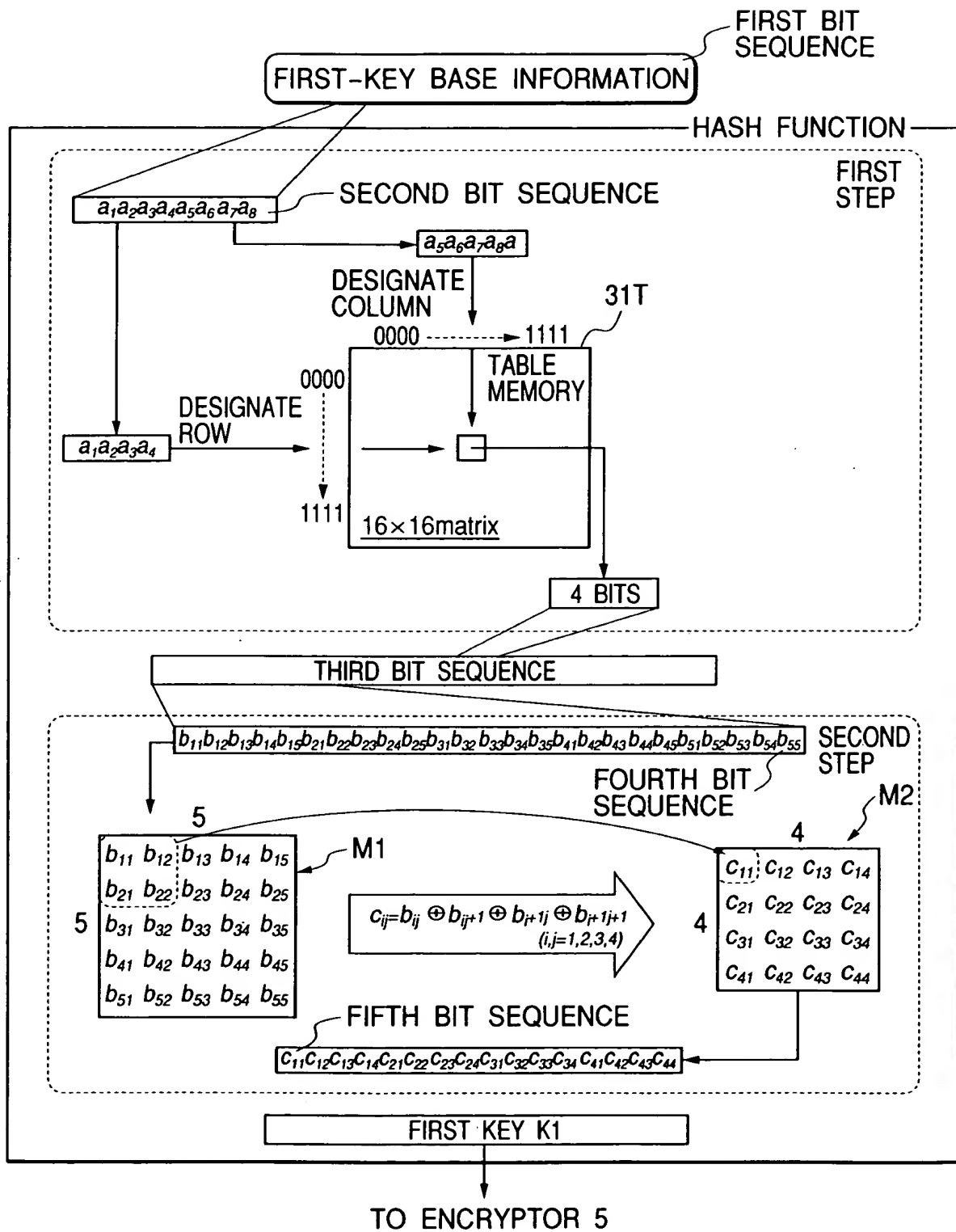


FIG. 6





7/7

FIG. 7

